IN THE CLAIMS:

Sub a1

1. A tamper resistant processor system, comprising:

a multi-component chip module (MCM) including:

a CPU;

one or more memory chips; and

one or more chip means containing at least one each of a de-encryption key and algorithm therein; and

an obscurant covering the contents of said multi-component chip module.

2. A tamper resistant processor system according to claim 1, further comprising said multi-component chip module in a bus configuration with other multi-component chip modules and said one or more memory chips.

3. A tamper resistant processor system, comprising:

processor boards;

an encrypted computer program;

a non-volatile memory, operatively connected to said processor boards, for storing said encrypted computer program and sending said encrypted computer programs to address destinations on said processor boards;

multi-component chip modules for receiving and de-encrypting said encrypted computer program and sending said de-encrypted computer programs to memory components on said multi-component chip modules.

4. A method for protecting a processor system from tampering, said method comprising the steps of:

a) mounting IC components on a single substrate as a multi-component module or as the contents of a multi-component module;

b) converting an encrypted computer program, received over a bus from a non-volatile memory, into its original un-encrypted form;

c) sending the de-encrypted computer program to appropriate locations in memory located in the multi-component module; and

d) protecting the multi-component module using one or a combination of an obscurant, deceptive patterns, and tamper detection/destruction mechanisms.

5. A tamper resistant processor system, comprising:

processor boards;

encrypted code;

a non-volatile memory, operatively connected to said processor boards, for storing said encrypted code and sending said encrypted code to address destinations on said processor boards; and

multi-component chip modules for receiving and de-encrypting said encrypted code and sending said de-encrypted code to memory components on said multi-chip modules.

6. A method for protecting a processor system from tampering, said method comprising the steps of:

a) mounting IC components on a single substrate a s a multi-component module or as the contents of a multi-component module;

b) converting encrypted code, received over a bus from a non-volatile memory, into its original un-encrypted form;

c) sending the de-encrypted code to appropriate locations in memory located in the multi-component module; and

d) protecting the multi-component module using one or a combination of an obscurant, deceptive patterns, and tamper detection/destruction mechanism.

7. A tamper resistant processor system, comprising:

processor boards;

encrypted data;

a non-volatile memory or network data source, operatively connected to said processor boards, for storing said encrypted data and sending said encrypted data to

address destinations on said processor boards and for receiving and storing encrypted data resulting from the processing of the input data; and

multi-component chip modules for receiving and de-encrypting said encrypted data, sending said de-encrypted data to memory components on said multi-chip modules, for storing the results of processing the de-encrypted data, and for encrypting the results before sending to storage or network external to the multi-component chip modules.

8. A method for protecting a processor system from tampering, said method comprising the steps of:

a) mounting IC components on a single substrate as a multi-component module or as the contents of a multi-component module;

b) converting encrypted data, received over a bus from a non-volatile memory, into its original unencrypted form;

c) sending the de-encrypted data to appropriate locations in memory located in the multi-component module;

d) encrypting processing result data that is being sent to storage or networks external to the multi-component module; and

e) protecting the multi-component module using one or a combination of an obscurant, deceptive patterns, and tamper detection/destruction mechanisms.

9. A tamper resistant processor system, comprising:

a multi-component chip module including:

a CPU; and

an in-line real time de-encryption chip;

one or more memory chips, operatively connected to said in-line real time de-encryption chip, said multi-component chip module encrypting out put to said one or more memory chips; and

a memory controller selecting between secured and un-secured memory over a processor buss.